"Method and system for the controlled delivery of digital services, such as multimedia telematics services"

======

The present invention relates to the controlled delivery of digital services such as multimedia telematics services, and it has been developed with particular attention to its possible application within the so-called OPIMA (Open Platform Initiative for Multimedia Access) initiative.

A description of the purposes and criteria that regulate this initiative is available as of the filing date of this application on the Internet site

http://www.cselt.it/ufv/leonardo/opima.

Further context information can be found for instance in the CENELEC EN 50221 standard, titled "DVB Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications", or in document DAVIC 1.3 Part 10: "Basic Security Tools for Davic 1.3", published in November 1997 on CD-ROM available from the DAVIC secretariat c/o Società Italiana Avionica S.p.A., Strada Antica di Collegno, 235, I-10146 Torino (Italy).

The invention however can find application in all the situations wherein a system is to be made that is able to allow a user to access, with a single decoder, coded information from different providers. The invention therefore can be employed in digital broadcast services via satellite or cable, for instance for the delivery of fee-payment audio-visual contents, even of interactive nature. A system according to the invention can be embodied within a decoder of the kind currently called Set Top Box (STB), within a personal computer, or integrated directly, for instance, in a receiver

such as a television receiver with digital interface.

Within this context, solutions have already been proposed and tested wherein access to the information (typically a television programme) requires the availability, at the user's premises, of a decoder device, essentially of a kind which is proprietary of the service provider. In other words, a certain decoder device allows receiving only the programmes transmitted by a certain service provider or, at most, by a limited number of providers adopting the same methods for delivering the services.

In general, to gain access to different providers, the user is however forced to obtain a multiplicity of different devices, using one or an other device as the case may be.

Attempts to attain a certain degree of standardisation have already been made, for instance through the definition, by the DAVIC International Forum, of the so-called CA0 interface and especially through the definition of the so-called CA1 interface, illustrated in detail in the DAVIC 1.3 document mentioned above.

Essentially, the aforesaid two interfaces operate at the two levels indicated respectively with dashed and dotted lines in the diagram in Figure 1, which is intended to illustrate both prior art solutions and the solution according to the invention.

In that diagram the references SP and U indicate respectively a provider of information services and a user thereof.

These services can be different information services, including (by way of non limiting example): audio and/or television programmes, in particular delivered according to different request and payment procedures, added value services, advertising services, also with prizes, services delivered upon subscription or coupon-based, various information services (banking and stock trading, road traffic, location, etc.), games, software distribution, remote sales, remote banking services, statistical survey services, also of interactive nature.

In the diagram in Figure 1, the reference D indicates the medium (broadcast via cable, via satellite, atmospheric, in a dedicated network, on Internet, etc.) through which the information generated by the provider SP reaches the reception system STB of the user U.

In the aforementioned DAVIC 1.3 standard, this information is already present in the form of an MPEG (acronym of Moving Picture Expert Group), data stream in particular as a stream encoded according to standard ISO/IEC 13818 (MPEG-2). Messages known as ECM and EMM, respectively, are inserted into this stream. The ECM acronym, which stands for Entitlement Control Message, identifies the control messages associated to a service. The EMM acronym, which stands for Entitlement Management Message, identifies instead the messages for managing the access

authorisations for services associated to a user.

Unit STU (i.e. Set Top Unit, which together with the security block indicated in its entirety as SD constitutes the receiving system STB available to user U) comprises in the first place a receiver block 100 destined to perform reception at the hardware level (demodulation, synchronisation, etc.) of the incoming data stream. The latter is destined to be sent to the block SD and in particular towards a filter 101 and a deciphering or decrypting block 102.

The signals sent according to the MPEG standard can be encrypted, thereby allowing them to be read in clear only by users enabled with an appropriate key.

The decrypting function is driven, within the unit STU, by the management module 103 which, through a respective control interface, sends instructions towards a module 104. The latter acts, within the block SD, as a so-called Security Manager. In practice, the function of the module 104 is to interact with the filter 101, with the deciphering or decrypting module 102 and with a user unit 105 to deliver towards the module 102 a deciphering key such as to allow the module 102 itself to decipher the incoming signal from the receiver 100. This signal can thus be rendered in clear and transferred to a demultiplexer 106 and to a decoder 107 (or to an equivalent processing chain) contained in the unit STU, in view of delivery to the user U.

In the more traditional systems mentioned above (of the kind implementing the so-called CA0 interface in current DAVIC terminology), the standardisation of the reception system STB in respect of the various SP service providers is limited to the unit STU alone.

All items below the dashed and dotted line which in Figure 1 identifies the interface CA0 constitute a part of device specialised according to a given service provider.

Adoption of the interface CA1 allows standardising the unit SD as well, shifting the need for specialisation to a lower level, i.e. the one of the user unit 105 which is to be made in removable form, in particular in the form of a so-called "smart card".

However, even the smart card construction fails to solve the problems summarised above, but simply transfers them to a different level. The user who desires to receive information from different providers SP will generally have to obtain many user units 105, thus many different smart cards, one for each provider. In addition to having to obtain multiple smart cards, the user should in any case reconfigure his reception system on each occasion depending on the provider of the services to be received, for instance by inserting the corresponding smart card into the system.

The rather impractical nature of such an operating procedure is evident,

especially considering that in a scenario like the one of the OPIMA initiative the intent is to provide the user with procedures for selecting the provider SP that are substantially similar to those normally adopted when receiving television programmes: in practice, the possibility of choosing provider and service through a simple action performed on a remote control set.

At least in principle, the drawbacks summarised above could be solved by providing for the insertion of multiple user units 105 in the reception system.

However, even independently of any consideration about the complexity of the system, this solution would still not solve the problem linked to the need, for the user, to obtain multiple user units 105.

The aim of the present invention therefore is to provide a solution that is able to avoid the drawbacks summarised above, in particular in relation to the possible adoption of the interfaces CA0 and CA1, while retaining general features of conformity with such interfaces.

According to the present invention, this aim is attained thanks to a method for service delivery having the characteristics set out specifically in the claims that follow. The invention further concerns the related system.

The invention shall now be described, purely by way of non limiting example, with reference to the enclosed drawings, wherein:

- Figure 1, representative - in general terms - also of prior art solutions, has already been examined above,
- Figure 2 shows, in the form of a functional block diagram corresponding to the OPIMA Reference Model, a possible embodiment of the invention, and
- Figure 3 shows, in the form of a flowchart, a possible operating sequence of a system according to the invention.

In Figure 2, elements identical or corresponding with those already described with reference to Figure 1 are indicated with the same references as in Figure 1. This applies in particular to the service provider SP, the delivery channel D towards the user U, the unit STU and the ideal location of the interfaces CA0 and CA1.

The whole of the functions shown with reference to Figure 1 referring to the modules 101, 102, 104 is carried out, in the diagram according to the invention of Figure 2, by a set of elements represented by the blocks TMW1, TMW2 and VM. The TMW acronym used for both blocks TMW1 and TMW2 indicates the fact that these blocks are normally realised at the level of the so-called "trusted middleware" (i.e. a software that performs security functions).

Briefly, the solution according to the invention can be seen as a development of the solution based on the interface CA1. In the solution according to the invention the

smart card 105, in addition to containing a cryptographic key that is not modifiable or legible from the outside, is able to receive, verify, store and execute an algorithm that allows using the services delivered by a given provider.

The verification phase aims at checking the authenticity and integrity of the algorithm before it is stored in the smart card, and it is based on checking a digital encrypted signature made by a Certification Authority recognised by service providers and by smart card manufacturers.

The execution of the service provider's specific algorithm allows deciphering the proprietary EMM/ECM messages of the service provider and to feed the deciphering module 102 which places the services required by the user in clear, thereby allowing their utilisation.

In this way the user will no longer need to obtain multiple units 105 in order to receive information from different providers.

According to the invention it is sufficient to have, for instance, a single universal smart card available, and specialisation information, necessary to receive a given provider's information in clear, can be downloaded directly from the system into the smart card, by exploiting its capability to execute the downloaded programs through its chip, and the software layer associated thereto, represented here as a virtual machine VM.

This gives the provider the further possibility to control and verify that a particular user actually has been enabled to receive certain programmes. Only after a given user has actually registered (for instance through a subscription) within the set of users authorised to receive a given service does the provider transmit the information that, processed at the level of smart card 105 level, allows the user to receive the service.

From the above it is readily apparent that, although it is preferred (for reasons better explained below) to embody the invention at the level of a movable support such as a smart card, the same function can be performed in a different way, for instance in the form of a circuit function comprised within the user system STB.

Unlike the interfaces CA0 and CA1 described above, which are intrinsically physical layer interfaces, the solution according to the invention is suitable for implementation at the programming layer, in particular by means of a smart card, such as, for instance, a so-called Java Card.

The terms "Java" and "Java Card" are registered trademarks of Sun Microsystems. The related description, in particular in regard to the definition of so-called APIs (the acronym stands for Application Programming Interface) is publicly available, as of the filing date of this application, at the Internet site

http://java.sun.com/products/javacard.

From this point of view, the solution according to the invention can be identified as a new interface layer, indicated in Figure 2 as CA2 for the sake of consistency with the references CA0 and CA1 used above, corresponding in practice to an intermediate layer of the user unit 105. In practical terms, the solution according to the invention provides for the so-called "trusted middleware" specified by the OPIMA reference model to be subdivided into a static part TMW1, included, according to the solution shown in Figure 2, within the STB module, and a dynamic part TMW2, included within the user unit 105.

The set of functions represented by TMW1 comprises, in particular, a module SP' whose function is essentially to extract a specific algorithm of the provider SP starting from the MPEG data stream coming from the receiver 100 (Figure 1) to load it into the user unit 105 as a specific part. Preferably, this algorithm is included as a private data stream in accordance with the aforementioned ISO/IEC 13818 standard. The remaining part in the set of functions TMW1 comprises the de-scrambler 102 and the related functions represented by the modules 101 and 104 in the diagram in Figure 1. The set of parts and functions TMW1 therefore is fully defined and wholly independent of the provider SP involved on the particular occasion and consequently is of a standardised type. In practice, the function indicated as TMW2 is identified by a specific algorithm of the individual provider SP which algorithm is downloaded into the user unit 105 in a secure manner (for instance because it is provided with cryptographic key) through the function SP'.

In this way the downloaded algorithm can be executed in the user unit 105 in a secure environment, thanks to the well known manipulation resisting features of smart cards.

This explains why, although in principle it can be embodied also by employing a circuit or a function incorporate in the user system STB, the solution according to the invention is preferably carried out at the level of a user unit 105 consisting of a smart card. This choice also allows an easy replacement of a smart card which may have been damaged or altered.

In use, when the user U chooses a particular provider SP (this can be done through a normal selection operation effected by acting on a remote control set) a so-called applet generated by the provider SP is transferred through the system STB for being loaded into the respective unit 105. As is well known, the term "applet" indicates a set of Java instructions that implements a given algorithm. Broadcast may take place, for instance, in case of radio broadcast transmission, by exploiting the carousel configuration adopted for broadcasting MPEG-2 DSM-CC (Digital Storage Media

Command Control Data). In this way, within the function TMW1, the filter 101 (Figure 1) is programmed in view of extracting the EMM data, specific for the individual user enabled.

The EMM messages can thus be read and deciphered in view of interpreting the data contained in the ECM messages. It is therefore possible to proceed with the extraction of the deciphering key CW relating to the service, which key is sent towards the de-scrambler 102, in order to allow the user U to receive the service through the demultiplexer 106 and the decoder 107.

Of course, it is also possible to envision additional functions, such as the one that provides for the secure transfer towards the provider SP of specific information about the service delivered, such as information pertaining to the usage of the service request.

A specific example of operation according to the general criteria outlined above is shown in the flowchart of Figure 3.

Starting from an initial step 200, the step indicated as 201 represents the choice of a particular provider SP by the user. This step can be effected, for instance, by tuning - in a way known in itself - the system STB on a certain frequency. As a result (step 202) the system STB starts receiving the data transport stream, for instance in the MPEG-2 format, transmitted by the provider SP.

The step 203 represents the extraction of the function TMW2 (of the dynamic type) by the function SP'.

After resetting (in the step 204) the user unit 105, in the subsequent step 205 the system STB loads thereinto (for instance as a Java Card applet) the function TMW2. The system STB then requests (step 206) the same unit 105, and in particular the virtual machine part VM which is able to process the extracted data, how to initialise the filter function, represented by the block 101 in Figure 1.

At this point (step 207) the system STB starts sending towards the user unit the filtered EMM data thereby completing the enabling of the provider/user communication. The user can then choose (step 208) the desired service. At this point the system STB starts filtering the ECM signals associated to the chosen service sending them towards the user unit 105 where it is checked (step 210) whether the user is authorised to access the service.

If the outcome is negative (unauthorised user), the operation progresses to another phase whereby another service may be chosen (step 216, to be illustrated farther on).

If, on the contrary, the user is found to be authorised (positive outcome of the comparison step 210) because he is registered as such with the provider SP,

particularly in relation to the selected service, the ECM data are deciphered by the unit 105 (step 211) and the respective control words are returned towards the system STB (step 212).

In this way the function TMW1 (static) of the system STB is able to decipher the service bringing it into the clear (step 213) in view of its delivery to the user (step 214) through the modules 106 and 107.

The step 215 is aimed at verifying whether the user, by applying a command (for instance imparted through a remote control set) to the system STB, expressed the will to interrupt use of the service or whether the service itself has ended.

If this is not the case (negative outcome of the step 215) the operation returns upstream of the step 211, with the possibility of taking into account a possible periodic variation of the deciphering key CW.

In case of positive outcome of the step 215, a subsequent step 216 is the verification as to whether the user intends to make use of a new service. As stated previously, the operation can evolve towards the step 216 also in case of negative outcome of the step 210, thereby allowing a user, who is not authorised to make use of a certain service, to choose a different service.

The negative outcome of the step 216 causes the evolution towards an end phase 300. It will be appreciated that this does not usually correspond to an actual turning off of the system STB but only to its reaching an idle state.

The positive outcome of the step 216 determines the return to the step 201 for the selection of a new provider or to the step 208 for the selection of a new service delivered by the same provider utilised previously, upon the outcome of a corresponding selection step 217.

Naturally, while the principle of the invention remains valid, the implementation details and the embodiments can be widely varied with respect to the description and illustration provided herein, without thereby departing from the scope of the present invention as defined in the claims that follow.